EXHIBIT I

An open letter to Google

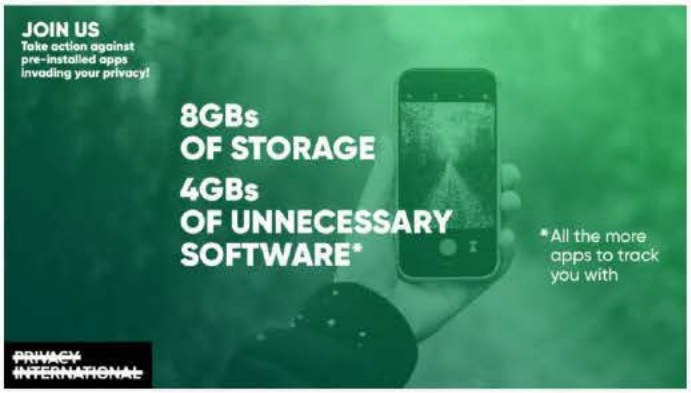
Privacy International and over 50 other organisations have submitted a letter to Alphabet Inc. CEO Sundar Pichai asking Google to take action against exploitative pre-installed software on Android devices.

KEY ADVOCACY POINTS

- Individuals should be able to permanently uninstall the apps on their phones. This should include any related background services that continue to run even if the apps are disabled.
- Pre-installed apps should adhere to the same scrutiny as Play Store apps, especially in relation to custom permissions.
- Pre-installed apps should have some update mechanism, preferably through Google Play and without a user account.
- Google should refuse to certify a device on privacy grounds, where manufacturers or vendors have attempted to exploit users in this way.

CONTENT TYPE
Advocacy

POST DATE
8th January 2020



You can find the letter below. **Add your voice to this campaign by signing our petition** if you believe that its time Google stopped enabling exploitation.

Note: This letter is also available in **French** and **Spanish**

Dear Mr. Pichai,

We, the undersigned, agree with you: privacy cannot be a luxury offered only to those people who can afford it.

And yet, Android Partners - who use the Android trademark and branding - are manufacturing devices that contain pre-installed apps that cannot be deleted (often known as "bloatware"), which can leave users vulnerable to their data being collected, shared and exposed without their knowledge or consent.

These phones carry the "Google Play Protect" branding, but **research shows that 91% of pre-installed apps do not appear in Google Play** – Google's app

TAGS

LEARN MORE
Poverty
Smartphones

OUR CAMPAIGN
Privacy shouldn't be a luxury

MORE ABOUT OUR PARTNER
Asociación por los Derechos Civiles
Centre for Intellectual Property and Information Technology Law
Coding Rights
Datos Protegidos
Digital Rights Foundation
Foundation for Media Alternatives
Fundación Karisma
Hiperderecho
Red en Defensa de los Derechos Digitales
TEDIC
The Institute for Policy Research and Advocacy (ELSAM)
Unwanted Witness

store.

These pre-installed apps can have privileged custom permissions that let them operate outside the Android security model. This means permissions can be defined by the app - including access to the microphone, camera and location - without triggering the standard Android security prompts. Users are therefore completely in the dark about these serious intrusions.

We are concerned that this leaves users vulnerable to the exploitative business practices of cheap smartphone manufacturers around the world.

The changes we believe are needed most urgently are as follows:

- Individuals should be able to permanently uninstall the apps on their phones. This should include any related background services that continue to run even if the apps are disabled.
- Pre-installed apps should adhere to the same scrutiny as Play Store apps, especially in relation to custom permissions.
- Pre-installed apps should have some update mechanism, preferably through Google Play and without a user account.
- Google should refuse to certify a device on privacy grounds, where manufacturers or vendors have attempted to exploit users in this way.

We, the undersigned, believe these fair and reasonable changes would make a huge difference to millions of people around the world who should not have to trade their privacy and security for access to a smartphone.

We urge you to use your position as an influential agent in the ecosystem to protect people and stop manufacturers from exploiting them in a race to the bottom on the pricing of smartphones.

Yours sincerely,

American Civil Liberties Union (ACLU)

Afghanistan Journalists Center (AFJC)

Americans for Democracy and Human Rights in Bahrain (ADHRB)

Amnesty International

Asociación por los Derechos Civiles (ADC)

Association for Progressive Communications (APC)

Association for Technology and Internet (ApTI)

Association of Caribbean Media Workers

Australian Privacy Foundation

Center for Digital Democracy

Centre for Intellectual Property and Information Technology Law (CIPIT)

Citizen D

Civil Liberties Union for Europe

Coding Rights

Consumer Association the Quality of Life-EKPIZO

Datos Protegidos

Digital Rights Foundation (DRF)

Douwe Korff, Emeritus Professor of International Law, London Metropolitan University and Associate of the Oxford Martin School, University of Oxford

DuckDuckGo

Electronic Frontier Foundation (EFF)

Forbrukerrådet // Norwegian Consumer Council

Foundation for Media Alternatives

Free Media Movement (FMM)

Freedom Forum

Fundación Karisma

Gulf Centre for Human Rights (GCHR)

Hiperderecho

Homo Digitalis

IJC Moldova

Initiative for Freedom of Expression- Turkey (IFox)

Irish Council for Civil Liberties

Media Foundation for West Africa

Media Institute of Southern Africa (MISA)

Media Policy and Democracy Project (University of Johannesburg)

Media Policy Institute (MPI)

Media Watch

Metamorphosis Foundation for Internet and Society

Open Rights Group (ORG)

Palestinian Center For Development & Media Freedoms (MADA)

Panoptykon

Paradigm Initiative

PEN Canada

Philippine Alliance of Human Rights Advocates (PAHRA)

Privacy International

Public Citizen

Red en Defensa de los Derechos Digitales (R3D)

Syrian Center for Media and Freedom of Expression (SCM)

TEDIC

The Danish Consumer Council

The Institute for Policy Research and Advocacy (ELSAM)

The Tor Project

Unwanted Witness

Vigilance for Democracy and the Civic State

RELATED CONTENT




PI response to UK Government consultation on Technical Capabilities Notices

Among the myriad of surveillance powers it already possesses, the UK government wants the power to stop companies – anywhere in the world – from making security improvements to their services without approval. To fall under this power, the company only has to service UK users, and yet the effects will be felt by every user, every where. CONTINUE READING

An open letter to TECNO Mobile

A coalition of 11 civil society organisations have called on TECNO to make serious changes to their practices protect users privacy and security. CONTINUE READING

How one TECNO phone is putting users' privacy and security at risk

Privacy International bought a TECNO smartphone, and we discovered serious concerns with the phone's operating system and pre-installed apps. CONTINUE READING

The cost of privacy: 3 years support for high-end Samsung phones, but what about the rest?

Samsung now offers 3 years of support for their most expensive models, but cheaper phones are still left out of the equation. CONTINUE READING